



정보화사회와 윤리

- 성신여자대학교 김도형 @ IT학부 -



제6장 인터넷 사기

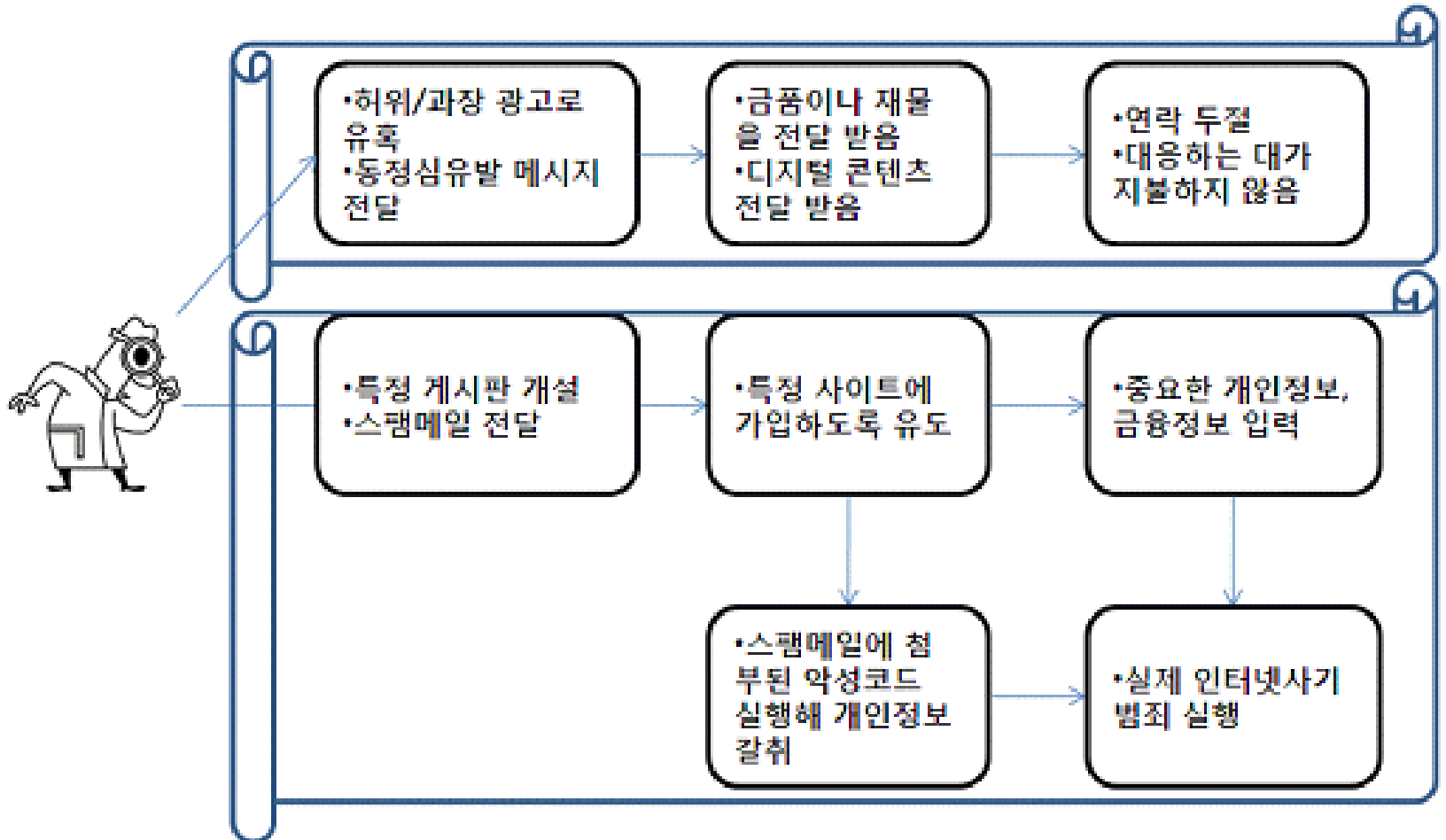
- 인터넷 사기의 정의
- 인터넷 사기의 유형
- 인터넷 사기의 실태
- 인터넷 사기의 사례
- 사전 대응방안
- 사후 대응방안

인터넷 사기의 정의 (1/2)

- 인터넷 사기란?
 - 정보통신망을 이용해 사용자들에게 물품이나 용역을 제공할 것처럼 기망하는 메시지를 보내서 금품을 부정하게 취득하는 사기행위의 한 유형
 - 인터넷 기술 자체가 가지는 특성인 익명성 보장과 정보의 누출이 용이하다는 단점 때문에 발생

인터넷 사기의 정의 (2/2)

- 인터넷 사기 절차



인터넷 사기의 유형 (1/5)

- 전자상거래(전자쇼핑몰) 사기
 - 인터넷 사기 중에서 가장 많은 부분을 차지하는 경우로서 전자 쇼핑몰에서 물품을 구입하고 대금을 지불하였으나 물품을 배송하지 않는 행위
 - 허위 물품 광고를 통해서 사용자가 구매한 물품과 다른 물품을 배송하는 행위

인터넷 사기의 유형 (2/5)

- 디지털 콘텐츠(게임 아이템) 사기
 - 온라인 환경에서 학습이나 기타의 목적으로 개발된 디지털 콘텐츠를 제공할 것을 약속하고 이에 대응하는 재물 혹은 이익을 취득한 후 제공하지 않는 행위
 - 온라인 게임에서 사이버 머니나 대응하는 대가를 취득하고 이에 대응하는 게임 아이템을 제공하지 않거나, 이와 반대로 게임 아이템을 제공 받은 후 대가를 지불하지 않는 행위

※ 현행법상 게임 아이템 거래는 불법

인터넷 사기의 유형 (3/5)

- 동정심 유발(구걸) 사기
 - 전자게시판을 사용해서 인터넷 사용자들의 동정심을 자극해 이익이나 재물을 취득하는 행위
 - 전자우편을 이용해 불특정 다수의 인터넷 사용자에게 동정심을 자극해 이익이나 재물을 취득하는 행위

인터넷 사기의 유형 (4/5)

- 피싱(Phishing)

- 공신력 있는 업체나 금융기관 등의 웹 서버를 해킹하여 위장 사이트를 개설하고 스팸 메일을 전송해 해당 사이트에 접속하게 한 후 개인정보나 금융정보 등을 취득하는 행위

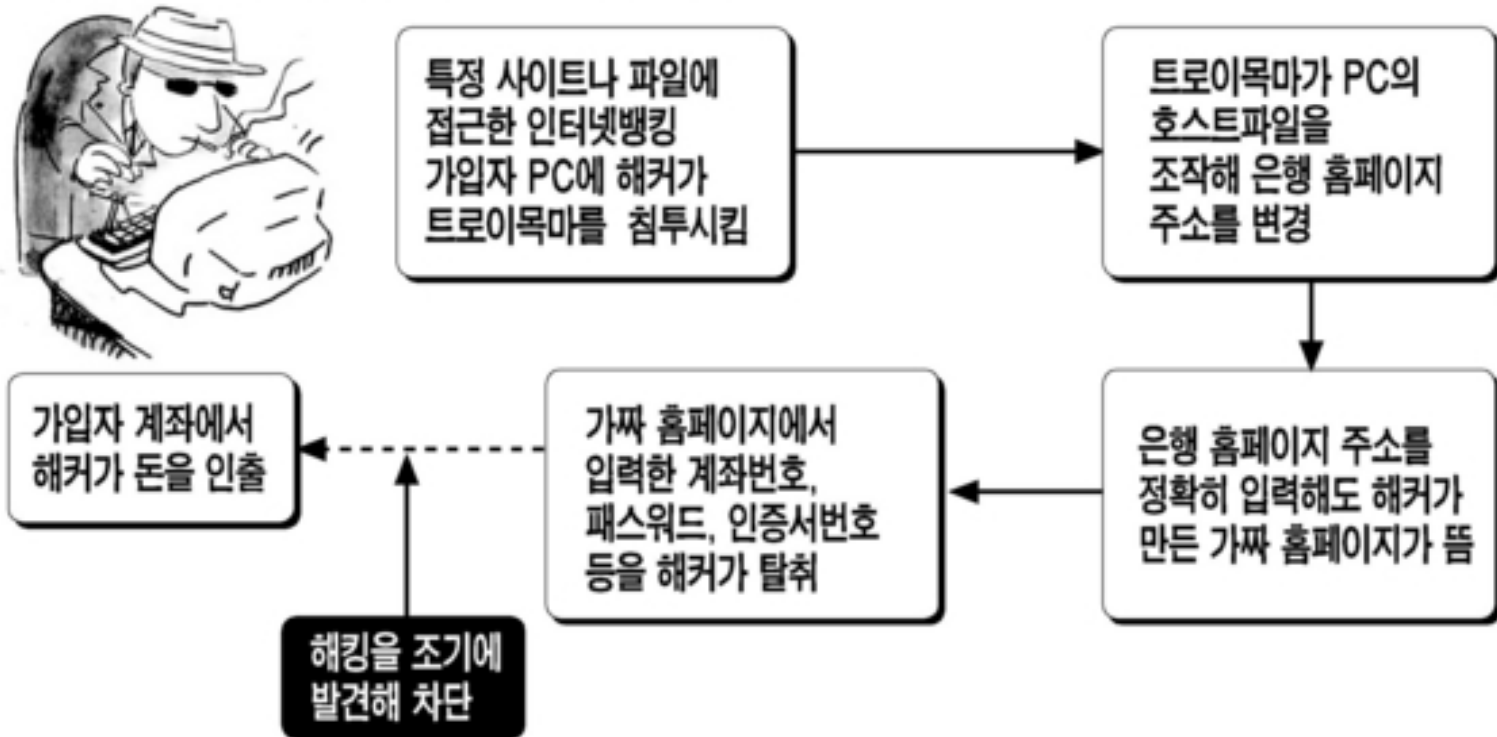
※ 개인정보(private data)를 낚시(fishing)하는 것처럼 낚아챌다는 의미에서 탄생된 용어로 은행사기(bank fraud) 또는 신용사기(scam); 금융기관이나 공공기관 사이트를 사칭하면서 사기행위자들이 의도하는 사이트로 연결시켜 개인정보를 빼냄으로써 직접적인 금융피해를 포함하여 개인정보를 악용할 가능성이 높은 사기 유형

인터넷 사기의 유형 (5/6)

- [파밍\(Pharming\)](#)

- 피싱이 발전한 수법으로 해당 웹 사이트를 중간에서 탈취하는 행위
← "phishing" + "farming"

국민은행 · 농협 인터넷뱅킹 해킹 흐름도



인터넷 사기의 유형 (5/5)

- 비싱(Vishing)

- 피싱이 발전한 수법으로 인터넷전화(VoIP)를 이용해 자동 녹음된 메시지를 보내어 은행 계좌에 문제가 있다는 식으로 경고하여 걱정하게 만들어서 계좌 비밀번호와 같은 중요 정보를 특정 중계기를 통해 입력하게 한 후 돈을 갈취하는 행위

- ← "Voice" + "phishing"

- ※ VoIP = Voice over IP

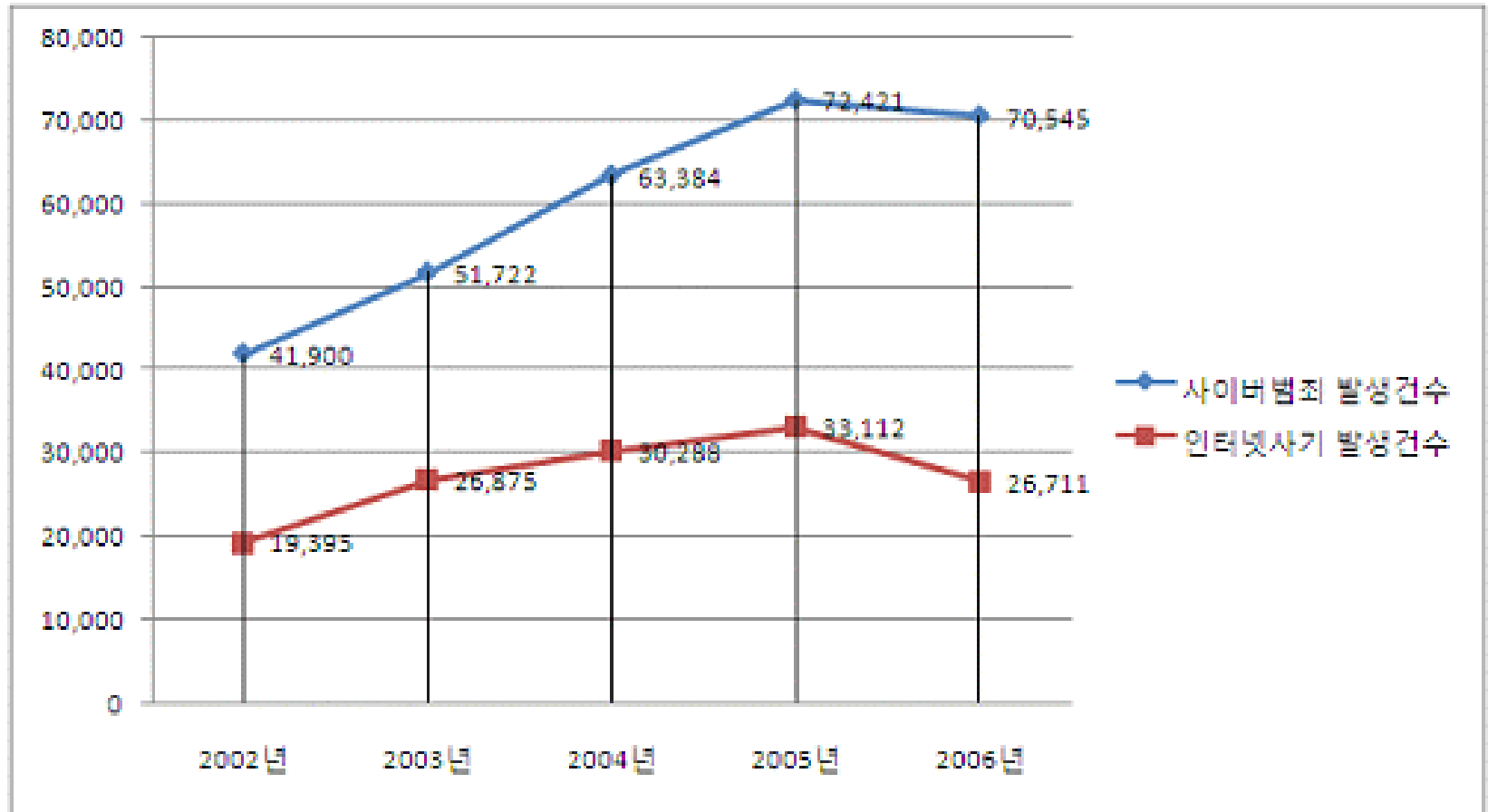
- 에스엠아이싱(SMishing)

- 휴대폰 문자를 발송해 악성코드가 존재하는 사이트로 접속하도록 유도한 후 휴대폰에 악성코드를 설치한 뒤 개인정보를 유출하는 행위

- ← "SMS" + "phishing"

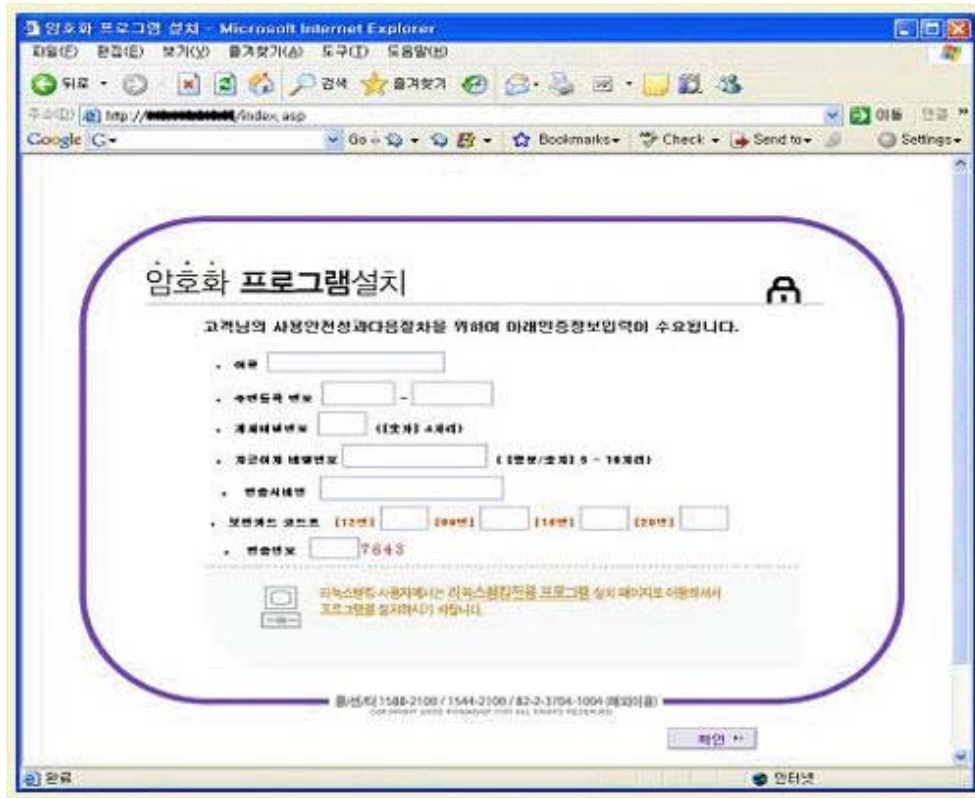
- ※ SMS = Short Message Service

인터넷 사기의 실태



인터넷 사기의 사례 (1/3)

- 피싱 사례



공신력이 있는 기관의 홈 페이지를 모방하여 홈 페이지를 개설하고 여기에 접속을 하도록 유혹한 후에 보안 서비스를 제공하기 위해서 암호화 프로그램을 설치한다는 안내와 함께 위와 같은 내용을 보여주고 개인정보를 입력을 요구한다.

인터넷 사기의 사례 (2/3)

- 비싱(보이스피싱) 또는 에스엠아이싱 사례 (1/2)

범죄자: 여보세요. xxx 님이시죠?

당신 : 네, 맞습니다. 누구신가요?

범죄자: 다름이 아니라, xxx님 당신의 부모님이 급하게 도로를 건너시다 제 자동차에 교통사고를 당하셨습니다. 지금 병원으로 모시고 왔는데 수술비를 입금하지 않으면 수술을 할 수 없다고 합니다. 생명이 위급하신 상태입니다.

당신 :?

범죄자: 부모님의 계좌번호인 000-11-222-1234로 수술비 100만 원을 입금하시고, 빨리 삼성동 xxx 병원으로 오시기 바랍니다.

당신 :?

인터넷 사기의 사례 (3/3)

- 비싱(보이스피싱) 또는 에스엠아이싱 사례 (2/2)

xx 텔레콤 안내원 박속여입니다. 고객님의께서는 현재 휴대전화 사용요금을 3개월 이상 연체하시어 10분 후부터 전화를 이용하실 수 없습니다. 이에 안내 메시지를 보내 드립니다. 이를 해결하고자 안내센터로 연결하고자 하신다면 고객님의 핸드폰 번호와 성명, 주민등록번호, 비밀번호를 입력하신 후 # 를 입력하시고 '통화' 버튼을 눌러 주시기 바랍니다.

xx 텔레콤 안내원 박속여
01x-114

'통화' <-- 연결하기

사전 대응방안 (1/8)

- 인터넷 사기 예방을 위한 개인 실천 사항 (1/5)
 - 전자쇼핑몰 사기
 - 해당 쇼핑몰의 신뢰성을 사전에 충분히 검토
 - 물품 판매자의 신원과 연락처 및 기본정보를 정확히 파악
 - 인터넷 거래 시 직접적인 거래보다는 검증된 사이트에서 간접 거래를 하는 것이 바람직
 - 인터넷 사기로 인해 피해를 입었을 경우를 대비하여 '거래 약관' 등을 자세히 살펴본 후 거래
 - 에스크로(escrow) 제도나 웹 사이트 인증제도 등이 적용된 안전한 쇼핑몰 사이트를 이용

사전 대응방안 (2/8)

- 인터넷 사기 예방을 위한 개인 실천 사항 (2/5)
 - 디지털 콘텐츠(게임 아이템) 사기
 - 개정된 정보통신망 이용 촉진 및 정보보호 등에 관한 법률에 따르면 게임 아이템의 현금 거래는 위법이므로 하지 않는다.
 - 사이버 상의 물품 교환이나 사이버 머니 기부 등은 공인된 중개사이트를 통해서 한다.
 - 학습 자료와 같은 디지털 콘텐츠를 구매하기 전에 안전한 에스프로 제도 등을 이용한다.

사전 대응방안 (3/8)

- 인터넷 사기 예방을 위한 개인 실천 사항 (3/5)

- 피싱

- 피싱이나 파밍 공격은 안전하지 않은 사이트로 도메인을 변경하거나 다른 웹 사이트로 연결하는 기술로서 해당 웹 페이지가 신뢰가 가지 않는다면 개인정보나 금융정보와 같은 중요 정보들을 한꺼번에 요청하는 경우에 입력하지 않는다.
- 피싱이나 파밍 공격을 위한 악성코드나 트로이 목마(Trojan Horse) 프로그램 등에 대해서 백신 프로그램 등을 사용하여 사전에 예방한다.

- 에스엠아이싱

- 휴대전화의 문자 메시지 등을 이용하여 은행의 지급기나 인터넷을 통해서 금융정보 등을 입력 요청시 사전에 침착하게 해당 기관에 사건의 사실 여부를 확인하고 처리한다.
- '연결하기'와 같이 특정 링크를 누르라는 요청에 대해서 응하지 않는다.

- 비싱(보이스피싱)

- 유·무선 전화를 통해서 ARS 등을 통해 음성 메시지를 수신한 경우 해당 내용을 꼼꼼히 듣고 이에 대해서 응답하기 전에 사실 여부를 명확히 확인한 후에 처리한다.

사전 대응방안 (4/8)

- 인터넷 사기 예방을 위한 개인 실천 사항 (4/5)
 - [한국정보보호진흥원](#) 10가지 수칙 (1/2)
 - ① 금융회사에서 제공하는 보안프로그램을 반드시 설치하기
 - ② 전자금융에 필요한 정보는 수첩, 지갑 등 타인에게 쉽게 노출될 수 있는 매체에 기록하지 않고, 타인(금융회사 직원 포함)에게 알려주지 않기
 - ③ 금융 계좌, 공인인증서 등의 각종 비밀번호는 서로 다르게 설정하고 주기적으로 변경하기
 - ④ 금융거래 사이트는 주소창에 직접 입력하거나 즐겨찾기로 사용하기
 - ⑤ 전자금융거래 이용내역을 본인에게 즉시 알려주는 휴대폰 서비스 등을 적극 이용하기

사전 대응방안 (5/8)

- 인터넷 사기 예방을 위한 개인 실천 사항 (5/5)
 - [한국정보보호진흥원](#) 10가지 수칙 (2/2)
 - ⑥ USB, 스마트카드 등 이동식 저장장치 보관
 - ⑦ PC방 등 공용 장소에서는 인터넷 금융거래를 자제하기
 - ⑧ 바이러스 백신, 스파이웨어(spyware) 제거 프로그램을 이용하고 최신 윈도우 보안 패치(patch)를 적용하기
 - ⑨ 의심되는 이메일이나 게시판의 글은 열어보지 말고, 첨부파일은 열람 또는 저장하기 전에 백신으로 검사하기
 - ⑩ 선수금 입금 요구, 상식수준 이상의 대출조건을 제시하는 경우 해당 금융회사에 동 대출 취급여부를 직접 확인하기

사전 대응방안 (6/8)

- 인터넷 사기 예방을 위한 제도적 접근법 (1/2)
 - 에스프로, 소비자피해보상보험, 채무지급보증, 공제계약 제도

구분	설명
에스프로 제도	소비자가 인터넷 쇼핑몰 등에서 인터넷 사기로 인한 피해를 입지 않도록 제3자(에스프로 사업자)가 소비자의 결제대금을 예치하고 있다가 상품배송이 완료된 후 통신판매업자에게 대금을 지급하는 거래 안전장치 (법률상 결제대금예치제도라 함)
소비자피해보상보험계약	통신판매업자는 소비자의 금전적 피해에 대하여 보상해 주는 것을 내용으로 사전에 보험회사와 보험을 계약하고 지급 사유가 발생한 경우 지체 없이 지급할 의무를 부여하는 제도
채무지급보증계약	통신판매업자는 소비자 피해보상금의 지급을 확보하기 위해서 금융기관과 채무지급보증 계약을 설정하고 이에 따라서 지급사유가 발생하면 즉시 지급하며 이를 지연할 경우 지연배상금을 지급해야 하는 의무를 부여하는 제도
공제계약	통신판매업자는 소비자 보호를 위해서 공제조합과의 공제계약을 설정할 의무를 부여하는 제도

사전 대응방안 (7/8)

- 인터넷 사기 예방을 위한 제도적 접근법 (2/2)
 - 옵트-인(opt-in) 제도
 - 전자상거래에서 인터넷 사기를 예방하기 위해서 관련기관은 옵트-인(opt-in)제도에 따른 규제 방법을 2005년 3월부터 시행하고 있다. 이는 전자우편, 전화, 팩스, 휴대전화 문자 메시지 등을 통한 광고성 정보(스팸 메일)을 규제하고자 기존의 수신자 거부 의사 타진 후에 발송 금지 조항(옵트-아웃; opt-out)과 반대의 개념으로서 광고를 보낼 때는 수신자의 사전 동의를 받아야 한다는 규칙
 - ※ 이메일 광고는 현재 적용되지 않음

사전 대응방안 (8/8)

- 인터넷 사기 예방을 위한 기술적 접근법
 - 피싱 예방을 위한 악성코드/스팸메일 퇴치 기술
 - 기술적으로 이러한 피싱 사이트들로부터 인터넷 사용자들이 안전할 수 있도록 악성코드나 스팸메일을 통한 정보 갈취나 엿보기 등을 사전에 예방할 수 있는 탐지 프로그램이나 차단 프로그램 등의 개발과 보급이 필요
 - 파밍 예방을 위한 인터넷 프로그래밍/도메인 관리 기술
 - 도메인 관리 업체가 관계 기관에서는 도메인 잠금 기능을 설정해 두고 온라인뿐만 아니라 오프라인 수단을 병행하거나 전자서명이나 공인 인증 기술과 같은 보다 안전한 인터넷 프로그래밍 기술들을 사이트에 적용해서 사이트의 안전성을 보장할 수 있도록 해야 한다.
 - 인터넷 사용자는 인터넷 브라우저의 보안성을 강화하기 위한 패치나 업데이트를 최신 버전으로 유지하기 위해서 노력하고 자신이 사용하고 있는 사이트를 늘 확인할 수 있는 DNS 운영 방식이나 도메인 등록 방식 등을 점검해 줄 수 있는 기술적인 해결책을 수용해야 한다.

사후 대응방안 (1/7)

- 인터넷 사기 관련 법률 (1/2)

- 사기죄(형법 제347조): 전자상거래에 있어서의 기망행위로 인한 부당한 재물 취득 금지
- 컴퓨터 등 사용 사기죄(형법 제347조의2): 컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령의 입력 등을 통한 부당한 재산상의 이익 취득 금지
- 절도죄(형법 제329조): 타인의 재물에 대한 절취 금지
- 컴퓨터 등 업무방해죄(형법 제314조2항): 컴퓨터를 이용한 타인의 업무 방해 금지
- 신용카드 부정사용죄(여신전문금융업법 제70조1항3호): 신용카드 부정 사용 금지
- 정보통신망 침해행위 등의 금지(정보통신망이용촉진및정보보호등에관한법률 제48조3항): 정보통신 침해행위의 제한
- 광고성 정보전송죄(정보통신망이용촉진및정보보호등에관한법률 제50조): 영리목적의 광고성 정보전송의 제한

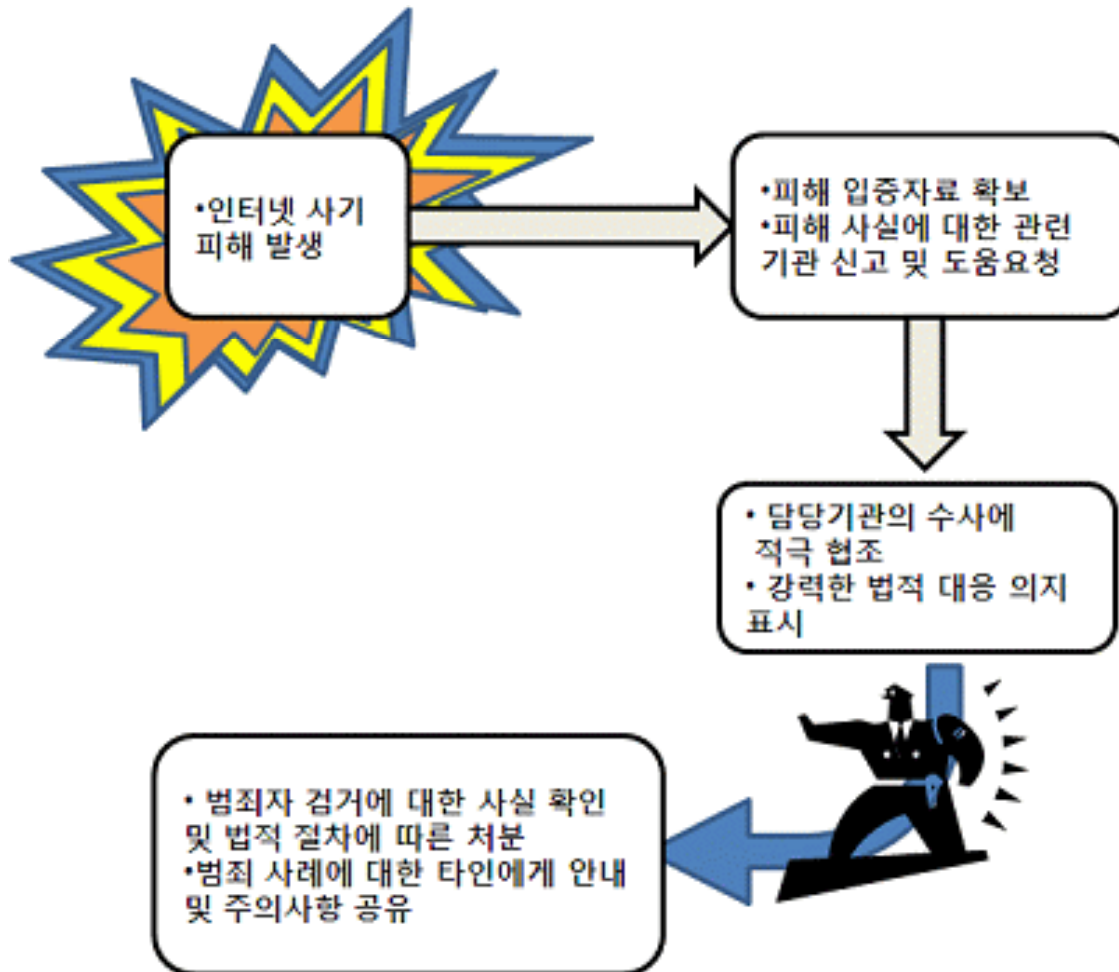
사후 대응방안 (2/7)

- 인터넷 사기 관련 법률 (2/2)

- 광고성 정보전송죄 과태료(정보통신망이용촉진및정보보호등에관한법률 제76조): 광고성 정보전송을 제한하기 위한 과태료
- 정보통신망 침해행위 등의 벌칙(정보통신망이용촉진및정보보호등에관한법률 제71조5호): 정보통신망 침해행위에 대한 벌칙
- 광고성 정보전송죄 벌칙(정보통신망이용촉진및정보보호등에관한법률 제74조): 광고성 정보전송을 제한하기 위한 벌칙

사후 대응방안 (3/7)

- 인터넷 사기 피해에 대한 일반적인 사후 처리 방법



사후 대응방안 (4/7)

- 사후 대처를 위한 사이트 (1/3)
 - 인터넷 사기피해 정보공유 사이트
 - <http://www.thecheat.co.kr>



사후 대응방안 (5/7)

- 사후 대처를 위한 사이트 (2/3)
 - 공정거래위원회
 - <http://www.ftc.go.kr>



사후 대응방안 (6/7)

- 사후 대처를 위한 사이트 (3/3)
 - 한국소비자원
 - <http://www.kca.go.kr>



사후 대응방안 (7/7)

- 기타 사이트

구분	사이트 주소
1. 한국정보보호진흥원	http://www.kisa.or.kr
2. 방송통신심의위원회	http://www.kiscom.or.kr
3. 사이버경찰청	http://www.police.go.kr
4. 경찰청, 사이버테러대응센터	http://www.netan.go.kr (http://www.ctrc.go.kr)
5. 경찰청, 사이버 112 (신고 / 제보 포털사이트)	http://cyber112.police.go.kr
6. 서울특별시 전자상거래센터	http://ecc.seoul.go.kr
7. 다단계 피해 감시센터 (안티피라미드)	http://antipyramid.org